AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with **tntgentlemansclub@icloud.com** that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014

Case No. 18-917M (NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1591(a)(2), 1952, and 1956.

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

FBI Special Agent Heather Wright
Printed Name and Title

Sworn to before me and signed in my presence:

Date: September 11, 2018

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Heather Wright, being first duly sworn, hereby depose and state as follows:

I. Agent Background & Experience

1. I am a Special Agent with the Federal Bureau of Investigation, and I have been so employed since July 2010.

2. As part of my duties, I investigate the illegal trafficking of persons for the purposes of labor and commercial sex acts. I gained experience in the conduct of such investigations through prior investigations, formal training, and in consultation with law enforcement partners employed by local, state, and federal law enforcement agencies. Prior to my assignment with the Milwaukee Division of the FBI, I worked in the pharmaceutical manufacturing industry as a Programmer Analyst for web applications from September 1999 through March 2001 and an Automation Engineer from June 2003 through July 2010.

3. The facts in this affidavit come from my personal observations, my training and experience, information obtained from citizen witnesses, and information reported to me by other law enforcement officers during the course of their official duties, all of whom I believe to be truthful and reliable.

4. Throughout this affidavit, "case agents" refers to the federal, state, and local law enforcement officers who have participated directly in this investigation, and with whom I have had regular contact regarding this investigation. The case agents in this investigation have included law enforcement officers from the FBI, Internal Revenue Service – Criminal Investigation, the Department of Labor – Office of Inspector General, the Dodge County Sheriff's Office, and the Hartford Police Department.

5. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. Purpose of Affidavit

6. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to requiring **Apple Inc.** ("Apple") to disclose records and other information, including the contents of communications, associated with the Apple ID **tntgentlemansclub@icloud.com**, stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, California. The warrant I seek would also authorize the government to search the information described below and in Attachment A for the things described in Attachment B.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

III. Probable Cause

A. Overview.

8. Case agents have been investigating Christopher Childs, Jennifer Campbell, and others for using force, fraud, and coercion to cause victims to engage in commercial sex acts. Childs currently is charged in Case No. 18-CR-69 (PP) with five counts of sex trafficking of adult victims by force, fraud, and coercion and one count of sex trafficking of a minor. Childs and Campbell (who served as Childs' "bottom" prostitute) also are charged with one count of conspiracy to engage in sex trafficking.

9. The investigation to date has revealed that Childs' sex trafficking activities typically took place in strip clubs located in Dodge County, Wisconsin, namely "The Hardware Store" in Clyman, Wisconsin, and "TNT," in Lebanon, Wisconsin.

10. The investigation to date has revealed that the owners, managers, and employees of TNT and the Hardware Store knew of, facilitated, and profited from Childs' sex trafficking offenses. The investigation is continuing into specific conduct by the clubs, their owners, and their employees, related to their interaction with and assistance to Childs and other pimps engaged in sex trafficking at the clubs. The investigation also is continuing as to possible money laundering and other financial crimes related to the proceeds of sex trafficking generated at the clubs.

B. Information provided by Victim 1.

11. On May 16, 2017, Victim 1, an adult female, reported to Hartford Police and the Dodge County Sheriff's Office that Childs was forcing and coercing her to be involved in commercial sexual activity. A short time later, Victim 1 made an additional statement about this conduct to me. Victim 1 reported that between October 31, 2015, and May 15, 2017, Childs regularly forced or coerced Victim 1 to perform prostitution dates, most often in the "champagne rooms" at TNT or the Hardware Store. Victim 1 further reported that Childs demanded that he be given all proceeds that she earned from prostitution dates and dancing at the strip clubs.

12. Victim 1 described Childs' rules when working at the strip clubs and performing prostitution dates. Victim 1 also described additional rules imposed by Childs that governed nearly every aspect of Victim 1's life. Victim 1 described the types of physical punishments that Childs inflicted on her for violating these rules and explained how Childs further threatened her by describing the punishments he had inflicted on past victims.

13. Victim 1 explained that at the end of every night, Childs required her to bring him all of the money that she had made. Initially, Victim 1 would have to drop the money off at Childs' residence every night on the way home from the strip clubs. The club managers would

provide payment to Victim 1 in a sealed envelope. Later, Childs installed a safe within Victim 1's home, and Victim 1 was to lock the envelope inside the safe. If there were any discrepancy as to how much money should be inside the envelope, Childs would call the club managers to verify how many times Victim 1, and other women working for Childs, had entered the champagne room.

14. Victim 1 stated that the owners and managers of both TNT and the Hardware Store were aware that Victim 1 and others were working for a pimp. According to Victim 1, the owners and managers of the clubs preferred to hire dancers with pimps because they would work any shifts required of them, show up on time, and bring in additional high-spending clientele who wanted to buy sex in the champagne rooms. Dancers with pimps generally had a greater motivation to earn as much money as they could because of their pimps' demands, and the club profited from this arrangement because they took a cut from each champagne room service. The club owners and managers also knew that they could call Childs if they had any problems with the women working for him and that Childs would deal with them right away.

15. Case agents have corroborated Victim 1's statements through other sources, including witness interviews, past complaints regarding TNT, the Hardware Store, and Childs, Facebook records, consensually recorded phone calls, and evidence found during the execution of search warrants.

C. Information provided by Victim 2.

16. On March 29, 2018, I spoke with Victim 2. Victim 2 corroborated Victim 1's statements regarding Childs and the strip clubs.

17. Victim 2 stated that Timothy Miller, while the manager of TNT, pretended to be nice to the girls working there; however, after Victim 2 had been working for Childs at TNT for

some time, Miller himself began acting like a pimp. Miller would set up prostitution dates between dancers from TNT and Radomir Buzdum, the owner of TNT. Miller would sometimes drive dancers to Buzdum's apartment in order for them to engage in prostitution activities. When Victim 2 attempted to leave Childs, Childs threatened to contact Miller and have Miller prevent Victim 2 from dancing at TNT or the Hardware Store. Victim 2 knew that Childs' girls made a lot of money for the clubs and that Miller would never agree to let Victim 2 continue to dance at TNT for fear that Childs would retaliate by pulling his other girls out.

18. Victim 2 also stated that Miller was involved in determining what prices the dancers in the club could charge for sex acts. She explained that Miller did not want any dancer charging less than a certain amount per "date" or for particular sexual acts because this would inevitably drive down the going rate, causing pimps like Childs to withdraw their top-earning girls from the club.

D. Information provided by CW-1.

19. On March 29, 2018, law enforcement involved in this investigation spoke with Cooperating Witness 1 (CW-1). CW-1 worked at TNT while Childs had his females dancing and doing prostitution dates at the club. In addition, CW-1 took over as club manager at TNT after Miller was fired in August 2017.

20. CW-1 stated that on a few occasions, Childs had approached CW-1 and told him that if CW-1 ever had any problems with the victims, Childs would take care of it. Childs also told CW-1 never to schedule "his girls" without first informing Childs, but that if CW-1 ever needed girls to fill the schedule, CW-1 should give Childs a call.

21. CW-1 stated that it was common knowledge among TNT's employees that Childs was abusive to Victim 1 and Victim 2. If either was out of line in any way, Childs' "bottom,"

who also danced at TNT, would report the matter to Childs. The next day, the victims would show up with better attitudes, but also with bruises all over their bodies.

22. On April 10, 2018, CW-1 provided additional information to law enforcement involved in this investigation. CW-1 described how TNT uses Facebook and other methods to recruit dancers and customers. CW-1 described how TNT pays its regular employees partially in cash, which was not reflected on payroll checks. CW-1 further described in detail how TNT profits from customers and dancers using the club's champagne rooms.

23. CW-1 explained that when Miller was managing TNT, the club was earning $15,000 to $20,000 per week. Each night the club was open, Miller or CW-1 would text the club owner, Radomir Buzdum, and his wife the sales figures for TNT, including a separate figure for the income from the champagne rooms. CW-1 explained that he typically texted these figures to the Buzdums at 10 p.m., 12 a.m., and closing.

E. Information provided by CW-2.

24. On April 19, 2018, I spoke with Cooperating Witness 2 (CW-2). CW-2 previously worked at TNT. CW-2 stated that Childs would occasionally visit TNT on weekends while his girls were working. CW-2 has overheard Miller speaking with Childs on the telephone and has heard Miller providing Childs with information regarding the number of champagne room visits Victim 1 and Victim 2 had made that night. Childs would verify how much money the victims had made and ask whether they had been drinking or had done any drugs.

25. CW-2 stated that it was common knowledge that Childs was abusive to his victims. In approximately February 2016, Victim 2 had disclosed to CW-2 that she could not get away from Childs. Victim 2 told CW-2 that Childs was physically abusive toward her and that she was frightened for her safety and the safety of her children.

26. CW-2 stated that CW-2 has walked into the champagne rooms at TNT on numerous occasions and seen dancers and customers completely nude. CW-2 knew that a champagne room service cost $200, which was split between the club and the girl. Usually, however, customers would pay $300-$400 in total because of addition of "extras" or "tips," which were tallied on a piece of paper and given to the girl at the end of the night in a sealed envelope.

27. CW-2 stated that Miller would allow drug dealers into the basement of the club, located near the entrance to the apartment which Miller stayed, providing an area for drugs to be sold. The club's dancers and regular customers often bought drugs there. CW-2 believed that Buzdum and Miller might have received a cut of the profits from the drugs sold within the club.

F. Information provided by Timothy Miller.

28. After Buzdum fired Timothy Miller in August 2017, Miller provided information to law enforcement about TNT's operations. Miller also provided law enforcement with handwritten notebooks that detailed TNT's various sources of revenue on a nightly basis, including the champagne room services.

29. Miller explained that although the champagne room was supposed to be for lap dances, "other things" went on there. TNT took a cut of the charge for the champagne room, but any other proceeds from the sexual activities that occurred within the champagne room were considered "extra" and negotiated directly between the dancers and the customers.

30. Miller stated that Buzdum was fully aware that TNT's dancers were performing acts of prostitution in the champagne rooms because Buzdum himself would pay for sex with the dancers. Buzdum had Miller give the dancers money for the sex acts out of TNT's income at the end of the night, and disputes would arise between dancers who were compensated disparately.

Miller provided a lengthy list of names of dancers whom he reported to have exchanged sex for money with Buzdum.

31. Miller explained that there are cameras located inside the champagne room for appearances but they are not recording. He stated that if police ever come to TNT and request surveillance footage, they are given tape that shows only the front door instead of the recordings of the inner areas of the club saved in an additional location inside the club.

32. Miller knew of several pimps who used to traffic their girls at TNT, including Childs and another pimp known as "Ball." Miller named several women who worked for each and specifically recalled that Ball's girls were "all beat up." Miller stated that he once saw a dancer receive $30,000 at the club from a prostitution customer and hand all of it over to "Ball."

33. Miller took care of the "books" for Buzdum and handwrote the figures of the daily income in notebooks according to source of revenue. Later, Miller began giving CW-3 the daily totals and having CW-3 keep the books.

34. Miller explained that he once lost one of the notebooks, and thereafter, he had CW-3 transfer all of the information from the various notebooks into one large notebook. CW-3 did not finish copying all of the information into the new notebook prior to Miller turning the notebooks over to me.

35. Miller stated that TNT earned a money through a variety of avenues throughout the night in addition to drinks and other items included in the "till," such as tip out from the dancers, lap dance and champagne room fees, and cover charge.

36. Miller stated he and Buzdum would communicate by phone throughout Miller's shift about how business was going and about the club's revenues. Miller estimated Buzdum easily earned $10,000 and up to $15,000 per week on gaming machines alone. Buzdum's

gambling machines were located within TNT and a tavern owned by Buzdum in Watertown, WI. The gaming machine income was not reflected in Miller's notebooks. Miller also stated that Buzdum did not report any of this income on his tax returns.

G. Information provided by CW-3.

37. I first spoke with Cooperating Witness 3 (CW-3) on October 12, 2017. CW-3 began working at TNT at age eighteen and generally was scheduled five days per week.

38. CW-3 was aware that Childs was a pimp who regularly brought his females to work at TNT. CW-3 stated that Childs' "bottom" danced under the name "Jada." I am aware that "Jada" is the name used by Jennifer Campbell. "Jada" would tell customers that Childs was not a pimp, however CW-3 and others knew this was not true. CW-3 never saw Childs hit "Jada," however "Jada" did whatever Childs told her to do.

39. CW-3 recalled that Victim 1 and Victim 2 both worked for Childs at TNT at the same time. CW-3 overheard Victim 1 tell others within the club on multiple occasions that Victim 1 wanted to leave Childs.

40. CW-3 explained that TNT got a "cut" of any champagne room fees. The regular price for a champagne room service was $200, and TNT would get half of that fee. Club employees, however, would regularly run customers' credit cards for amounts like $500 and provide customers the difference in cash so that they could negotiate and pay for sexual services directly with the dancers.

41. If there were any issues with any of the girls working at the club, Miller or CW-1 would have to deal with the issue.

42. CW-3 recalled that Buzdum would get drunk and have sex with the dancers at TNT. Buzdum would tell these women that he was going to pay them and then either pay them less than what he promised or not pay them at all.

43. On August 13, 2018, I met with CW-3 again. CW-3 said that CW-3 started out cleaning TNT after hours when CW-3 was too young to be in the club during business hours. When cleaning the champagne rooms at TNT, CW-3 often would find used condoms, condom wrappers, tissues, and wet wipes littered all over on weekends or busy weeknights.

44. After turning 19 (in 2012), CW-3 began working as a bartender at the club. Buzdum would often arrive at the club drunk. Buzdum would drink more when he arrived, then pay one or more of the females at the club for sex. Buzdum would usually select from the same group of dancers each time and would direct the bartender to pay the dancer after the sex act. Buzdum would pay the dancer anywhere from $200 to $1,000 out of the club's cash till.

45. According to CW-3, Campbell was one of the females whom Buzdum paid for sex. At first Buzdum did not know that Campbell worked for a pimp. Even after Miller explained the situation to him, however, Buzdum continued to pay Campbell for sex.

46. CW-3 would assist Miller with tallying money and sending income information to Buzdum via text message at the end of the night. When Buzdum and his wife, Dawn Buzdum (referred to as "Dawn" for clarity), filed for divorce, Dawn began seeking information about TNT's earnings. Buzdum had CW-3 purchase and set up a cell phone for TNT in order to send the "official" nightly numbers to himself and to Dawn simultaneously via a number associated with the club. In fact, however, Miller texted Buzdum the club's full and accurate nightly earnings in a separate message that Dawn did not receive.

47. CW-3 set up an iCloud account and a Facebook account associated with the cellular number of the TNT phone purchased by Buzdum. CW-3 backed this account up to her computer. CW-3 stated that the iCloud account was **tntgentlemansclub@icloud.com** and the phone number associated with the account was **(920) 988-6855**. CW-3 was the only person who had access or the password to the iCloud account. When CW-3 left TNT in August 2017, CW-3 had Buzdum sign a contract to have the phone switched into his name. CW-3 "wiped" the phone from her laptop.

48. On September 6, 2018, based on CW-3's information, I caused a preservation request to be served on Apple for all records relating to the account associated with the Apple ID **tntgentlemansclub@icloud.com.**

H. Information regarding Apple.

49. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be used through numerous iCloud-connected services and can store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-

connected device. For example, iCloud Mail enables a user to access email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share images and videos with other Apple subscribers.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

f. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers.

50. Apple services are accessed through an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services.

51. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address or an email address associated with a third-party email provider. The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID.

52. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account, the methods used to connect to and utilize the account,

the Internet Protocol ("IP") address used to register and access the account, and other log files that reflect usage of the account.

53. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

54. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service.

55. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by

Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can be decrypted by Apple.

56. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. For example, stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity. In this case in particular, CW-3 set up an Apple ID of **tntgentlemansclub@icloud.com** for the phone TNT used to contact and text income figures to the owner of TNT and his wife. These figures specifically included totals from unlawful sexual activity taking place in the club's champagne rooms.

57. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a

search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account.

IV. Probable cause to search TNT's iCloud account.

58. As explained in Section III above, there is probable cause to believe that Childs has engaged in sex trafficking involving force, fraud, and coercion, and that TNT, its owners, and it managers benefitted financially from participation in a venture that involved sex trafficking, in violation of Title 18, United States Code, Section 1591(a)(2). There is also probable cause to believe that, knowing prostitution was taking place in the champagne rooms and collecting a cut of each service, TNT and its owners and managers, laundered the proceeds of that unlawful activity by comingling those proceeds with TNT's other income, in violation of Title 18, United States Code, Section 1956. Finally, there is probable cause to believe that TNT and its owners and managers used facilities in interstate commerce, such as cellular phones and credit card readers, to promote, manage, and carry on prostitution activity unlawful under Wisconsin law, in violation of Title 18, United States Code, Section 1952.

59. Based on the evidence detailed in Section III, there also is probable cause to believe that the iCloud account associated with Apple ID **tntgentlemansclub@icloud.com** contains evidence related to these crimes, including text messages sent in interstate commerce regarding the nightly proceeds being generated from prostitution activities occurring at TNT.

V. Conclusion.

I respectfully submit that this affidavit establishes probable cause for the issuance of a warrant to search the Premises described in Attachment A, and for the seizure of the evidence described in Attachment B.

ATTACHMENT A

Premises to be Searched

This warrant applies to information associated with **tntgentlemansclub@icloud.com** (the "account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., 1 Infinite Loop, Cupertino, CA 95014.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information is within the possession, custody, or control of Apple, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

d. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iCloud Tabs, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

e. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

f. All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

g. All records pertaining to the types of service used;

h. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

i. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be seized by the government.

All information described above in Section I that constitutes evidence or instrumentalities of violations of Title 18, United States Code, Sections 1594(b) (conspiracy to engage in sex trafficking), 1952 (use of facility in interstate commerce to promote, manage, or carry on unlawful prostitution activity), or 1956 (money laundering), from 2012 to the present, including:

a. All information and communications in any form, including text messages, instant messages, emails, and other forms of messages concerning the operations of TNT Gentleman's Club, including the scheduling of dancers, nightly revenues at TNT, amounts that dancers had earned or were owed by TNT, negotiations with dancers' "handlers" or "pimps," and other club-related business, whether legal or illegal;

b. Photographs or videos of dancers or strippers, the interior or exterior of TNT, the staff of TNT, or any other image related to the operation of TNT;

c. All call and messaging logs;

d. Contact lists, to assist with the interpretation of the communications documented in the call logs and to identify the parties listed as affiliated with TNT;

e. Evidence of user attribution, showing who used or owned the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, notes, documents and Internet browsing history;

f. Evidence of use of third-party apps and websites, such as Facebook, related to the offenses under investigation;

g. The identity and location of the persons who have used the Apple ID;

h. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;

i. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and

j. Evidence that may identify any co-conspirators, aiders and abettors, or victims including records that help reveal their whereabouts.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.